CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0319

Insider Trading Threats on Dark Web and Underground Sources

Insikt Group used the Recorded Future® Platform, the dark web, and OSINT sources to investigate the existence of insider trading groups among financially motivated cybercriminals and retail trading communities. This report will be of interest to financial institutions, governments, and law enforcement agencies seeking to understand the influence of these groups on the stock market.

Executive Summary

Insider trading can be carried out more easily now than ever before, due largely to the continuing proliferation of encrypted and anonymous messaging services, and the existence of dark web and underground communities that allow threat actors to find co-conspirators and communicate with them. Historically, a small number of dark web forums catered to the trafficking of non-public corporate information; now, updated technology allows for these efforts to be conducted with much greater operational security. Financially motivated threat actors or disgruntled employees can now exchange information away from the prying eyes of law enforcement and security researchers, allowing only vetted individuals to access sensitive data being provided by insiders.

Additionally, the clearnet is host to many market trading enthusiast groups, on places like Reddit and Discord. These groups range in size from thousands to millions of users. Their existence provides a recruitment vector for threat actors operating insider trading groups, and moderators of these legitimate clearnet communities would likely not be fully capable or have the will to curtail such efforts. Insikt Group also discovered "stock signals" services, providing paid users with tips on which trades to make based on the recommendation of "analysts". Given that the origin of the information is unclear, the unregulated nature of these services and the use of anonymous messaging services is concerning. The use of messaging services that allow anonymous registration by these services creates a scenario where, if illegal activity is taking place, it would be very difficult for law enforcement and private sector security professionals to trace the real world identities of users.

Key Judgments

- Historical examples of dark web advertising for insider trading indicates a strong demand for non-public information sharing. Motivated threat actors will take advantage of this demand.
- Forums catering to insider trading have disappeared as threat actors migrate to more secure and anonymous messaging platforms.
- Clearnet stock trading communities provide lucrative opportunities for insider trading group organizers to recruit new members.
- Large and unmonitored stock trading discussion groups present unique security challenges to publicly traded companies.

Background

Typical cyber threat discussions of dark web activities tend to center on the sale of compromised payment card data and other financial information, trafficking of personally identifiable information (PII), distribution of malware and malware-as-a-service (MaaS), laundering and cashout services, and other overt fraud. These products, along with the enormous illicit substances market, make up the largest pillars of dark web forums and market activities. In fact, some of the most visited dark web sites are dedicated exclusively to these specific items and services. However, other less frequently discussed security threats also exist. One of these topics is insider trading and recruiting of insiders. There have been instances of insider trading being organized by dark web forum users in past years, reported primarily in 2017. However, the sources referenced in much of that reporting, specifically KickAss Market and The Stock Insiders, have been out of operation for some time. Insikt Group also found little current reporting on such activities, despite this historical precedent. It is not likely that cybercriminals would simply abandon efforts to acquire or monetize insider information, given the potential profit. This leads us to the prediction that this activity is still taking place, but advances in technology and the operational security of threat actors may have pushed it further underground, making it more challenging to detect. This research effort is intended to test these predictions, and to ascertain the current threat landscape for insider trading on dark web or clearnet sources.

This research focuses on findings of insider trading activity and recruiting from Recorded Future's dark web source collection. Insikt Group points out how common these activities are and where such activities take place. Insikt Group's research involved two phases: Phase one involved passive investigations using key words in the Recorded Future Platform. Phase two involved active human intelligence collection with the objective of organically gathering information that was not available on publicly viewable threads. This phase included conversations with human sources close to or heavily involved in clearnet stock trading communities.

Additionally, we pivoted from what was observed, and analyzed possible vectors of insider trading that could plausibly be active using dark web forums as well as encrypted and secure communications methods like Signal and Telegram. We believe, based on previous investigations and dark web monitoring, that insider trading communities likely exist, but such communities are using a high degree of operational security to hide their activities. Central to this assessment is the historical precedent for the creation of dark web communities that have accommodated insider trading activity, The Stock Insiders and KickAss Market being the most prominent examples.

Additionally, while not directly related to insider trading and the sharing of non-public information, but indicative of the potential power of online financial communities, clearnet stock trading communities have been covered heavily in the news media over recent activities. One Reddit-based group that Insikt Group researched heavily, known as Wall Street Bets, coordinated the mass purchases of a number of stocks, primarily GameStop and AMC. This caused the prices of these companies to skyrocket, while putting hedge funds who had been heavily shorting these stocks (predicting a continuing price decline) to potentially lose billions of dollars. The news of this activity became increasingly divisive as the finance community began to suggest regulation, and popular retail stock trading platforms for individual and small cap investors such as Robinhood took the unprecedented step of halting trading on these stocks. Some reports also implicated disinformation and bot-driven campaigns being carried out on Wall Street Bets. Following these events, online stock trading groups will likely be more heavily scrutinized by government agencies as well as the financial industry going forward.

Underground Trading Communities

Current Landscape

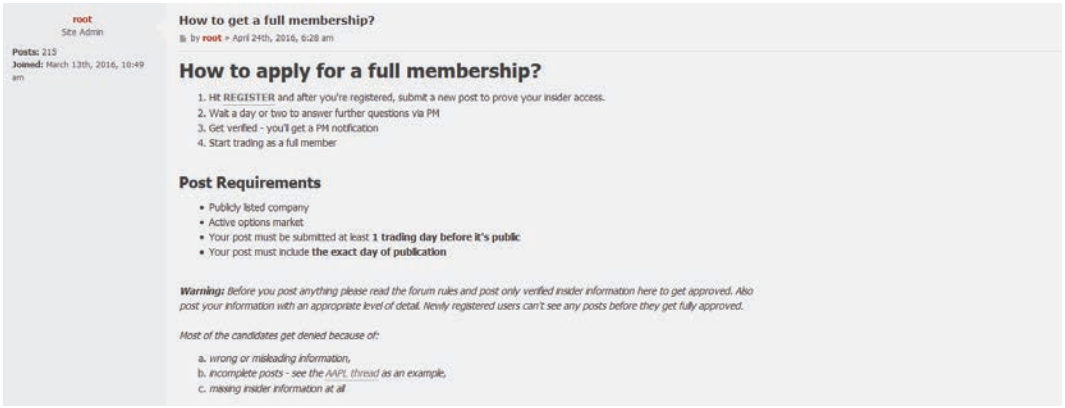
Regardless of the historical precedent for insider trading communities being operated on the dark web, we did not find any communities for sharing or discussions of non-public corporate information on threads currently in operation. While insider trading might be referenced, we did not observe threat actors actually coordinating efforts, claiming to have made stock trades based on non-public information, or seriously recruiting users with insider knowledge for the purposes of stock trading. While it is possible that posts have been made outside the research window or using imprecise language that was not collected in our searches, these references are certainly not pervasive or common.

However, this is not to say that discussions of stock trading in general are uncommon, or that legal activities that could quickly turn to illegal activities are not being discussed with regard to stock trading. There are numerous posts advertising tutorials on how to make money trading stocks, as well as advertisements for stock signals groups (basically, paid subscriptions to services that recommend selling or buying stocks based on forecasting and past data). In addition to dark web references, searches in open sources showed that there are stock trading communities on Reddit with millions of subscribers, such as r/WallStreetBets and r/Investing. These communities also have associated Discord servers in some cases.

The Stock Insiders

One of the historically relevant sites had been The Stock Insiders, a Tor-based website, active from April 2016 until August 2018. As the name suggests, the website was created with the intent of having a community of users with insider access at publicly traded companies who would be willing to share it with other users in order to inform the stock trades of the larger group. The website has long been inactive, the administrator is not responsive to private messages, and there have not been any updates to the main page since early 2018. The reason that operations ceased has not been explained but it does not appear to be the result of a law enforcement takedown since the website is still technically up.

While the site is no longer active, it still provides an instructive view of how its operations were carried out. The Stock Insiders has a few viewable posts instructing users about how to register an account and listing out the requirements for full membership, which is based on providing verifiable non-public information prior to public release, although exactly what type of information is not specified. It appears that the website allowed newly registered members to make posts to a more open forum, and if they were deemed worthy of membership they would then be invited to a closed part of the forum where non-public information was freely exchanged for all full members. The website also states that users had the option of selling non-public information directly to the forum, presumably by making a deal directly with the administrators, although it is said explicitly that the user must give the information first and when it is verified (by the news being publicized) they will receive a payment based on how much the stock price of the company in question changed.



root
Site Admin
Posts: 215
Joined: March 13th, 2016, 10:49 am

How to get a full membership?
by root » April 24th, 2016, 6:28 am

How to apply for a full membership?

1. Hit REGISTER and after you're registered, submit a new post to prove your insider access.
2. Wait a day or two to answer further questions via PM
3. Get verified - you'll get a PM notification
4. Start trading as a full member

Post Requirements

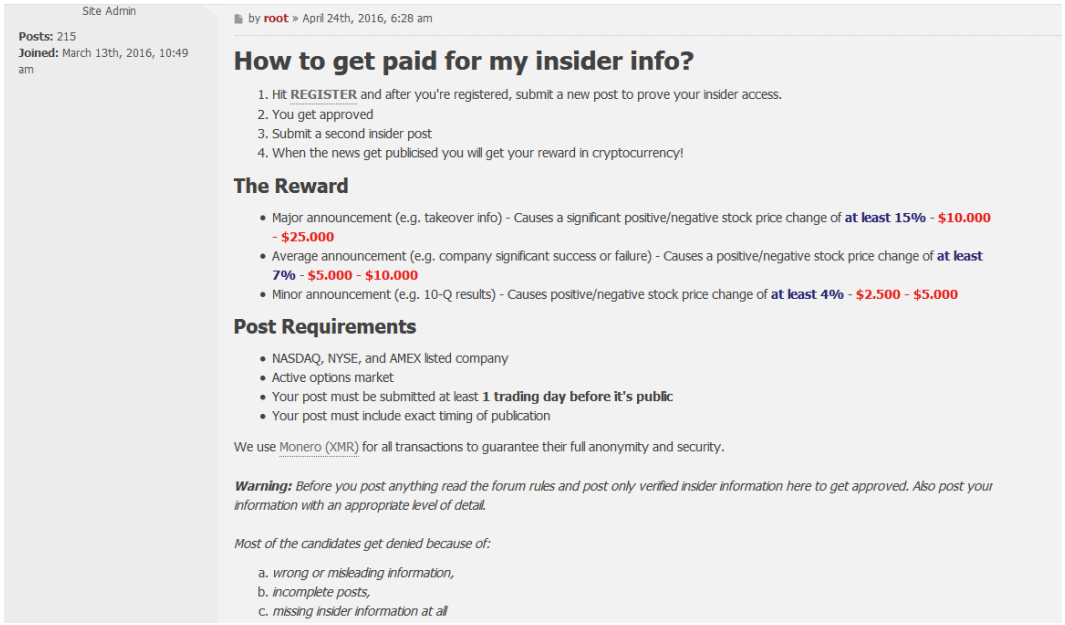
- Publicly listed company
- Active options market
- Your post must be submitted at least **1 trading day before it's public**
- Your post must include **the exact day of publication**

Warning: *Before you post anything please read the forum rules and post only verified insider information here to get approved. Also post your information with an appropriate level of detail. Newly registered users can't see any posts before they get fully approved.*

Most of the candidates get denied because of:

a. *wrong or misleading information,*
b. *incomplete posts - see the AAPL thread as an example,*
c. *missing insider information at all*

Figure 1: Welcome post made by the administrator of The Stock Insiders



Site Admin
Posts: 215
Joined: March 13th, 2016, 10:49 am

by **root** » April 24th, 2016, 6:28 am

How to get paid for my insider info?

1. Hit REGISTER and after you're registered, submit a new post to prove your insider access.
2. You get approved
3. Submit a second insider post
4. When the news get publicised you will get your reward in cryptocurrency!

The Reward

- Major announcement (e.g. takeover info) - Causes a significant positive/negative stock price change of **at least 15%** - **$10.000 - $25.000**
- Average announcement (e.g. company significant success or failure) - Causes a positive/negative stock price change of **at least 7%** - **$5.000 - $10.000**
- Minor announcement (e.g. 10-Q results) - Causes positive/negative stock price change of **at least 4%** - **$2.500 - $5.000**

Post Requirements

- NASDAQ, NYSE, and AMEX listed company
- Active options market
- Your post must be submitted at least **1 trading day before it's public**
- Your post must include exact timing of publication

We use Monero (XMR) for all transactions to guarantee their full anonymity and security.

Warning: *Before you post anything read the forum rules and post only verified insider information here to get approved. Also post your information with an appropriate level of detail.*

Most of the candidates get denied because of:

a. *wrong or misleading information,*
b. *incomplete posts,*
c. *missing insider information at all*

Figure 2: More instructional information posted by the administrator of The Stock Insiders

KickAss Market

Another historically important but defunct forum, KickAss Market, was a hacking forum used by capable and motivated threat actors and operated from February 2016 to January 2019. This source stood apart from other underground sources because it was known to have a very high standard for entry, requiring prospective users to prove their cyber intrusion skills to be granted access. It was also somewhat distinct at the time as the operators offered courses in cyber intrusion methods to newer, less experienced members.

The marketplace was reported as enabling the transmission of non-public information from companies so that users could profit from informed stock trades. According to reporting from 2019, KickAss Market users also participated in the sale of network access, hacking, coding, and malware sales.

While according to sensitive sources there have been intermittent rumors of its impending return, KickAss Marketplace has been defunct since early 2019, after a sudden shutdown that was likely an exit scam carried out by the administrators. An exit scam in this context refers to the administrator of an underground market closing the site suddenly and keeping the funds held in user wallets or escrow deposits for themselves. This sudden shutdown may have been prompted after a threat actor called The Dark Overlord (TDO) stated publicly that he had shared information related to 9/11 terrorist attack victim insurance claims, which he gained access to by hacking Hiscox Insurance Company. The operators of KickAss Market may have been trying to avoid blowback from highly controversial data being shared on their website and the public being made aware of it.

Stock Signals

While searching for insider trading references across dark web sources, 1 relevant result was detected, on Hack Forums. Insikt Group discovered a post advertising a service called “Astro Trader” that operates the website astrotrading[.]io and a payment portal where customers can pay with a credit card or in cryptocurrency. There is cause for concern based on how this business and others like it are operated. The actors involved are anonymous, and while there is no specific evidence of non-public information being shared, the contributors to these services could be working for one of the companies they make stock recommendations on, or more likely, working in finance positions that give them access to data on a myriad of publicly traded companies and are using that to inform their stock signals. Astro Trading is advertised as providing the following services for a $60 monthly fee:

- “A wide variety of guides that enable you to learn the science behind options trading”
- “Consistent analysis on many stocks from notable analysts”
- “Weekly watchlists from our analysts that enables members to an understanding of how each analyst trades”
- “Consistent profitable plays”
- “Seminars for beginners to experts provided by our analysts”
- “Trading bots that cost $200 alone”

Recorded Future sources obtained a license for the service to determine what type of information was being discussed or whether there were any signs of illegal activity on the service. Once the server was accessed, we observed posts made by “analysts” who provided stock market tracking information as well as suggestions on stocks to buy and ones to avoid. There were channels on the server where users were posting screenshots of gains being made using past tips given by analysts on the server, as well as another channel in which users posted screenshots of stock trades that resulted in loss of value. From what we observed, the analysts, who are likely running the service, appear to be at least knowledgeable about the practice of market trading. At the time of this writing there were several hundred users online in the Discord server. We did not observe anything to indicate that non-public information is being used to generate these stock signals, but there was no explanation as to where the information is coming from, and we were not able to review all the information posted in depth as it is a very active server.

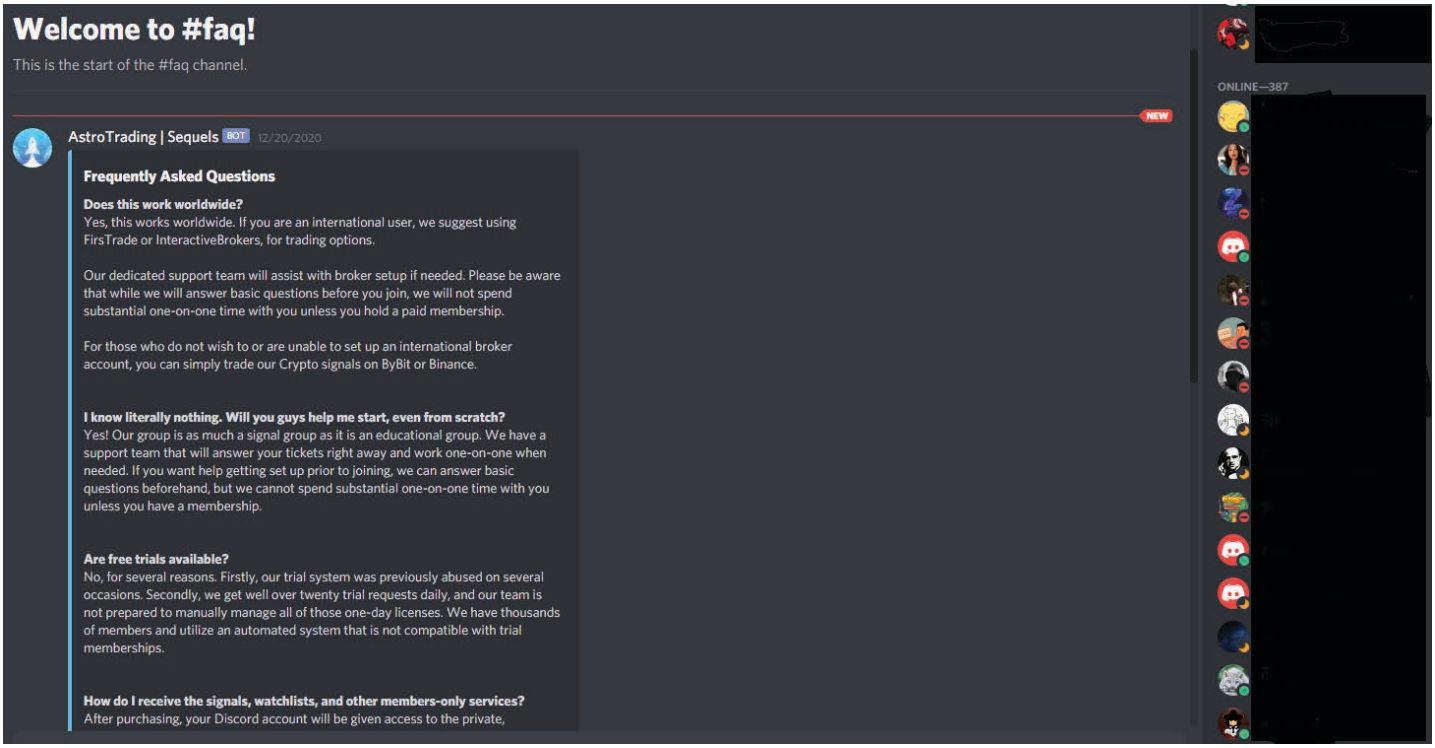
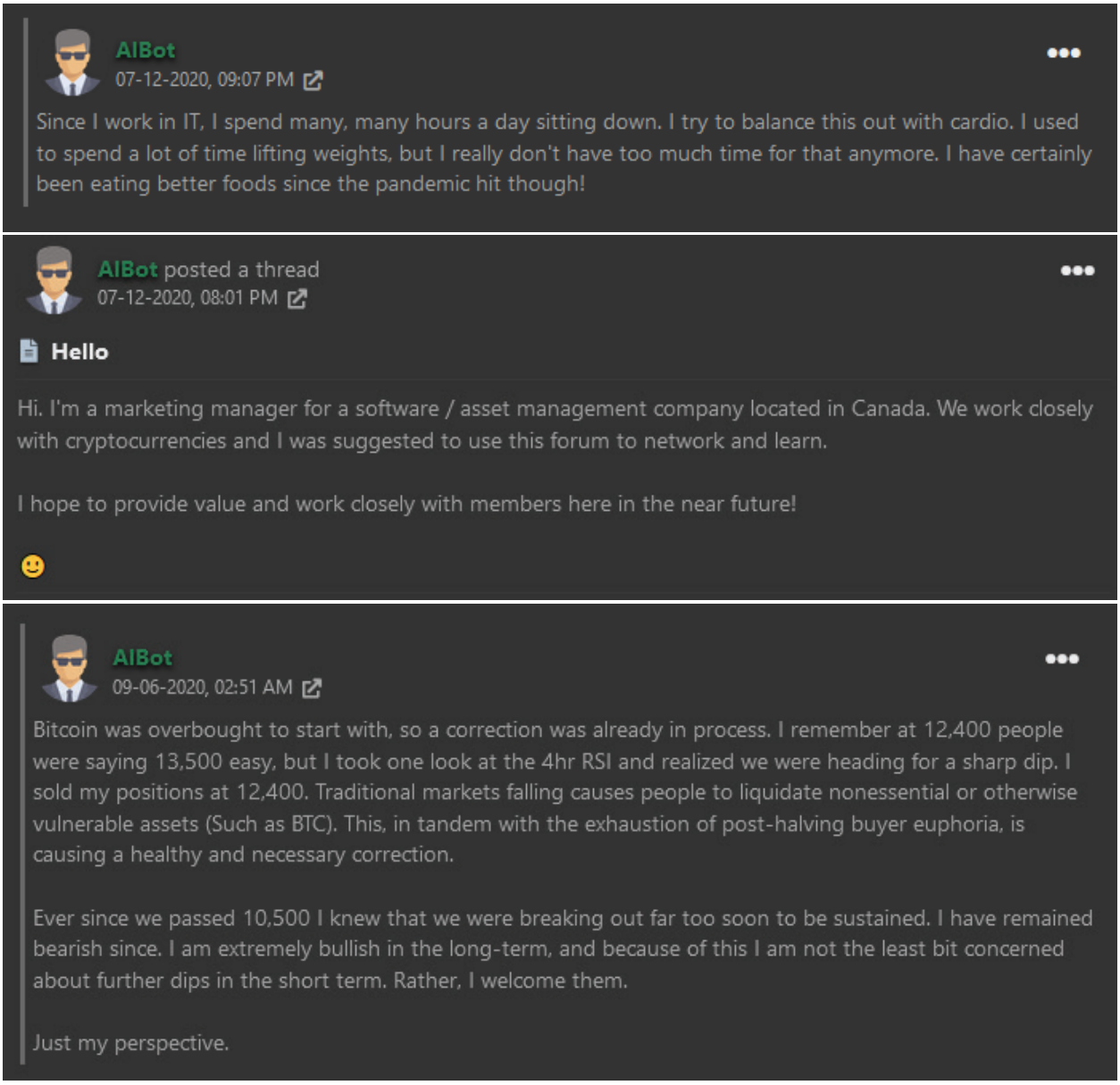


Figure 3: FAQ from Astro Trading group Discord server

There is also a question of why this service would be advertised on a hacking forum. While overt criminal activity discussion is against the rules of Hack Forums, sale of compromised online gaming accounts and discussions of various scamming techniques are common. One particular user on Hack Forums that has made posts regarding Astro Trading is AIBot. AIBot has only been on the forum since July 2020 and has made a low number of posts and a few dozen comments in that time. Most of the comments were unremarkable, with a select few being related to stock trading and cryptocurrency investment but not pertaining to anything illicit. However, in several comments, AIBot mentions that they work in information technology (IT), and more specifically, as a marketing manager for a software and asset management company in Canada. This is not direct evidence of illegal activity, but it does demonstrate that it is plausible that operators of Astro Trading are giving stock advice based on non-public information they can access through their jobs — in this case, information held by the unnamed software and asset management company this forum member is employed by.



Figures 4, 5, 6: Posts made the Hack Forums by "AIBot", who advertises Astro Trading services

Posting on Hack Forums demonstrates at least a possible willingness on the part of Astro Trading operators to assist cybercriminals in leveraging ill-gotten gains. The completely unregulated nature of this service shows how this type of platform could be adapted for criminal activity.

Options Trading Discussion Groups

A number of clearnet communities were found in which users discuss options trading, particularly Reddit and Discord, of which servers were founded for discussions of options trading. The most prominent of these sources are the subreddits r/WallStreetBets and r/Investing, communities with just over 9.5 million and 1.7 million subscribers at the time of this writing, respectively. There are also associated servers hosted on the popular chat application Discord, with several hundred members online at any given time, in channels for options trading and international market discussion, as well as a number of social channels.

r/WallStreetBets

The community r/WallStreetBets has been getting a significant amount of media coverage in recent days after it appeared that the group coordinated the purchase of a massive amount of shares of the publicly traded stock of video game retailer GameStop. The stock of the company was being widely shorted by several hedge funds which enabled members of WallSteetBets to, in some cases, make very large profits when the coordinated efforts sent the stock skyrocketing from under $20 dollars per share in mid-January 2020 to, briefly, $483 a share on January 28, 2020. While this is not related to the issue of insider trading, it illustrates the size of some of these communities and their power to potentially influence the market in ways that some experts deem borders on the illegal. These events should put clearnet stock trading communities on the radar of publicly traded companies.

These communities have rules against the sharing of non-public information, and after analyzing new posts, no suspicious activity was observed. In an effort to gather more information, Insikt Group researchers communicated with moderators of the Discord servers for r/WallStreetBets and r/Investing and sought clarification about their policies regarding insider trading. These communications included requests for information about specific actions that were taken to enforce any applicable policies. In response to these attempted communications, the r/WallStreetBets Discord server moderators blocked our account. A moderator of the Discord for r/Investing was more responsive, but after an extended back and forth declined to provide any substantive information. The moderator expressed concern that the information they provided might be used against the Discord server's users.

The refusal to cooperate with these research efforts is not evidence that the moderators of these communities allow or are complicit in any insider trading activity. Although it is likely that if there had been recruitment efforts taking place in those communities (even activity that is banned and removed) the moderators would have simply replied and stated that no insider trading-related discussion was observed on their server. It is probable that users have attempted to solicit non-public information or to recruit other users for insider trading and the moderators don't want that to be known as it would potentially put their legitimate Discord servers and Reddit communities at risk. These Discord communities are not as visible as clearnet forums, and would therefore be a more subtle place for potential organizers of insider trading efforts to recruit. This highlights the position that encrypted and more anonymized chat services have in cyber threat landscapes, and likely in the insider trading threat landscape specifically. Even if recruitment attempts and solicitation of non-public information have not taken place within these communities before, it is worth highlighting that these communities would be good places to target these efforts as they are populated with many users who know how to trade options, and in many cases likely work in finance and for publicly traded companies.

Future Threat Analysis

The existence of communities that enable users to anonymously discuss stock trading raises concerns. Threat actors looking to monetize their own non-public information or interested in creating a community for similarly motivated insiders would pursue one of two avenues based on our observations and predictive analysis. The first would be the creation of a sales platform where information can be sold or traded for a share of future proceeds. The second is a closed trading group where only vetted insiders can share information with each other without money changing hands.

Direct Purchase Source

A threat actor could choose to set up a marketplace that would serve as a platform where insiders could advertise and sell information gathered from the company they work for that could be valuable to those who might wish to profit off of a movement in a stock price after the information being offered becomes public.

There are a number of problems with this type of direct sale scenario:

- Non-public information is not something that can easily be assigned a dollar value. How much the information might impact a stock price is not a simple task, and even if it can be predicted, the profit potential then depends on how much the purchaser has to invest in the stock. These factors would make assigning a price that users are willing to pay and also makes the risk worth while for the insider challenging.
- Non-public information cannot be verified until it is publicly released, and once it is publicly released, the stock price impact is apparent almost immediately. This means that a buyer has to trust the provider of non-public information, making gathering first-time customers very challenging.
- There is also the obstacle of reaching users that are actually interested in stock trading using insider information, which will probably be a niche audience on most underground forums. This is because most threat actors on those platforms are interested in direct profit activities such as carding and other fraud. Some examples of this would be Verified Forum, one

of the most prominent sources for carders, and Omerta Forum, another long standing community that allows users to traffic in compromised credit cards, personally identifiable information, and compromised e-commerce accounts. However, if a motivated threat actor can provide a platform that offers carders reliable profit potential and reasonable security, a portion of them might try to leverage their ill-gotten gains through illegally informed stock trades.

- The final, and probably most important issue, is that of law enforcement observations. If a website was created that was openly advertising the sale of non-public corporate information, it would only be a matter of time until law enforcement agencies either discovered it themselves or were alerted to it by researchers who monitor underground sources. Once that happens, law enforcement could pose as a prospective buyer and even purchase information themselves to verify the existence of a legitimate insider threat. The company the insider works for can then be notified and an investigation can begin which would very likely discover the insider and lead to an arrest. There is plenty of precedent for law enforcement monitoring dark web sources that host criminal activity and seizing the site when enough evidence is gathered and often arresting administrators and users. A recent example of this was the September 2020 global action against Wall Street Market, which resulted in 179 arrests and the seizure of large caches of drugs and cryptocurrency.

All of these potential problems combine to make this scenario of insiders selling their information directly to other parties fairly unlikely, and if it were to be set up, it would not be likely to persist for very long.

Closed Trading Group

Given the challenges of the direct sale model, the most likely avenue for malicious insiders to trade information would be within a trusted group. Group members could offer their information in exchange for membership to a group of other malicious insiders, all of who are contributing non-public information from their respective companies. In effect, the insiders, instead of directly profiting, can make profitable stock trades of their own using information provided by the other members who have access to information from companies that they would never have had access to before public release.

This scenario would have a number of advantages and circumvent many of the challenges of the previously explained direct sale scenario:

- It overcomes the challenge of pricing as there are no funds changing hands. The information holder does not need to haggle over price or deal with complaints and possible refund requests.
- Users do not have to set up cryptocurrency infrastructure or means of cashing out that cryptocurrency and accounting for that income.
- This system could also employ a trust system to screen out possible law enforcement efforts. The most effective would be to require proof of insider access and a willingness to share information. While there could be a number of benchmarks, perhaps the most effective would be requiring a prospective member to provide earnings information prior to public release, in the form of hard numbers or an SEC form.
- The operator of a closed trading group would also have the opportunity to tightly control recruitment efforts, possibly using sources like those on Reddit and Discord. Using these sources or similar ones as recruiting grounds would allow the group operator to decide who to reach out to, specifically based on their activity in those communities, and converse with them before giving the location of the closed group or even disclosing that it exists until they have an idea of the likelihood the potential recruit would be receptive. Additionally, since the group operator is recruiting specific users, this decreases the chances that they will inadvertently draw the attention of law enforcement.

If setup and recruitment efforts were successful and a group operator was able to organize even a dozen insiders with access to sensitive corporate data and willingness to share that information with each other, the potential profit that could be earned could be substantial. Additionally, a group of people, each individually sharing their insider information but not making stock trades on it themselves would represent a very difficult investigative challenge unless the group was infiltrated by investigators. Even if infiltration was successful,which could be a challenge all its own if the barrier to enter is strict enough, the identity of users might be difficult to ascertain if the group operator takes sufficient steps to provide anonymity.

Outlook

Insikt Group's discoveries during the course of this research demonstrate that while insider trading may not be the type of criminal activity that some threat actors are interested in, there is likely enough demand for groups catering to it to function. It is likely that this activity has migrated to encrypted and anonymized chat services, as opposed to remaining on publicly accessible dark web or underground forums. We believe those sources will continue to be where this type of activity is conducted as they provide enhanced operational security for threat actors.

There are inherent challenges to operating an insider trading group on a forum that is not accessible by non-members, such as issues of generating and directing enough traffic to the group, but it is possible for motivated group organizers to recruit from legitimate stock trading discussion groups on sources like Reddit and Discord. Those groups are populated by users who are highly profit driven and many take significant financial risk. Furthermore, Insikt Group's interactions with moderators of those communities do not inspire confidence that action against recruitment for something like an insider trading group would be immediately taken.

Insikt Group recommends security professionals focus on detecting recruitment efforts not only on dark web sources but on clearnet market trading communities targeting insiders at their organization or client organizations. For law enforcement, we recommend broad monitoring for any recruitment efforts, for insiders in general and specifically for references to closed market trading groups.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.